Appl. No. : **09/787,784**
Filed : **July 30, 2001**

AMENDMENTS TO THE CLAIMS

Claims 1-8 are canceled.

9. (currently amended) A data transfer system comprising:

a key facility;

a sender facility configured to communicate with the key facility, the sender facility ~~including~~comprising:

_____a first encryption module configured to encrypt data for an intended recipient, wherein ~~to provide~~ a first encrypted part and a remaining encrypted part are produced, the first encrypted part carrying information for decryption of the remaining encrypted part ~~so~~such that the remaining encrypted part ~~cannot~~ be decrypted ~~without~~ only after decrypting the first encrypted part;~~, a partitioning module to split the data into encrypted parts such that no part is decryptable on its own,~~

_____a second encryption module configured to encrypt ~~at least one of the parts for a third party~~ the first encrypted part so as to produce a ~~further~~ third encrypted part, ~~which is~~ the third encrypted part being decryptable only by the key facility;~~,~~

_____a combiner configured to combine the ~~further~~ third encrypted part ~~and a~~with the remaining encrypted part to produce a data block, and

_____a first transmitter configured to send the data block; and

a receiver facility configured to communicate with the key facility, the receiver facility ~~including~~comprising:

_____a receiver configured to receive the data block;~~,~~

a splitter configured to split the data block into the third encrypted part and the remaining encrypted part; and

a command module configured to generate a request for the key facility to decrypt~~ion of~~ the ~~further~~ third encrypted part, wherein the first encrypted part is recovered, ~~by the key facility,~~ the receiver further adapted to receive the first encrypted part from the key facility;

wherein the key facility further comprises:

a first decryption module configured to decrypt the third encrypted part ~~, on~~after receipt of the request from the receiver facility, ~~the further third encrypted part~~ wherein ~~to reveal~~ the first encrypted part is recovered; and

a second transmitter configured to send ~~it~~ the first encrypted part to the receiver facility; and

wherein the receiver facility further comprises a second decryption module configured to decrypt the first encrypted part so as to ~~thereby~~ enable the subsequent decryption of the remaining ~~and the decrypted further~~ encrypted part ~~provided by the key facility~~.

10. (currently amended) The system of Claim 9, wherein the sender facility includes a signature module to sign the data block.

11. (currently amended) The system of Claim 9, wherein the first transmitter is configured to send the data block to the key facility, and wherein the key facility further includes a receiver configured to receive the data block and to forward the data block to the receiver facility.

12. (currently amended) The system of Claim 11, wherein the key facility further includes a log module configured to log receipt of the data block.

13. (currently amended) The system of Claim 9, wherein the receiver facility is configured to communicate with the key facility and the sender facility, and wherein the first transmitter is configured to send the data block to the receiver facility, the receiver facility further ~~including~~ comprising a receiver to receive the data block.

14. (currently amended) The system of Claim 13, wherein the key facility further ~~includes~~ comprises a log module configured to log receipt of the ~~further~~ third encrypted part.

15. (currently amended) The system of Claim 9, wherein the key facility further ~~includes~~ comprises a log module configured to log receipt of the request for decryption of the ~~further~~ third encrypted part as proof of delivery of the data block to the receiver facility.

16. (currently amended) The system of Claim 15, wherein the sender facility further ~~includes~~ comprises a delivery module configured to request proof of delivery information from the key facility.

17. (currently amended) The system of Claim 9, wherein the key facility is a trusted third party. ~~is the key facility.~~

18. (currently amended) A method of data transfer, comprising:

at a sender facility:

encrypting data for an intended recipient, wherein ~~to provide~~ a first encrypted part and a remaining encrypted part are produced, the first encrypted part carrying information for decryption of the remaining encrypted part sosuch that the remaining encrypted part cannot be decrypted ~~without~~only after decrypting the first encrypted part;~~,~~

~~splitting the data into encrypted parts such that no part is decryptable on its own,~~

encrypting ~~at least one of the parts for a third party~~the first encrypted part to produce a ~~further~~ third encrypted part, the third encrypted part being ~~which is~~ decryptable only by the key facility;~~,~~

combining the ~~further~~ third encrypted part ~~and a~~with the remaining encrypted part to produce a data block, and

sending the data block;

at a receiver facility:

receiving the data block; ~~and~~

splitting the data block into the third encrypted part and the remaining encrypted part;~~,~~ and

generating a request for the key facility to decrypt the third encrypted part;~~requesting decryption of the further third encrypted part by a key facility;~~

at the key facility:

decrypting the third encrypted part, ~~on~~ after receipt of the request from the receiver facility, ~~the further third encrypted part to reveal~~ wherein the first encrypted part is recovered, and

transmitting the ~~decrypted further~~first encrypted part to the receiver facility;

and

at the receiver facility:

receiving the first encrypted part from the key facility; and

decrypting the first encrypted part so as to ~~thereby~~ enable the subsequent decryption of the remaining ~~and the decrypted further~~ encrypted part ~~provided by the key facility~~.

19. (previously presented) The method of Claim 18, further comprising signing the data block at the sender facility.

20. (currently amended) The method of Claim 18, wherein the sending at the sender facility ~~is configured to send~~comprises sending the data block to the key facility, and wherein the method further comprises at the key facility receiving the data block and forwarding the data block to the receiver facility.

21. (previously presented) The method of Claim 20, further comprising, at the key facility, logging receipt of the data block.

22. (currently amended) The method of Claim 18, wherein the sending at the sender facility ~~is configured to send~~ comprises sending the data block to the receiver facility, and wherein the method further comprises, at the receiver facility, receiving the data block.

23. (currently amended) The method of Claim 22, further comprising, at the key facility, logging receipt of the ~~further~~ third encrypted part.

24. (currently amended) The method of Claim 18, further comprising, at the key facility, logging receipt of the request for decryption of the ~~further~~ third encrypted part as proof of delivery of the data block to the receiver facility.

25. (previously presented) The method of Claim 24, further comprising, at the sender facility, requesting proof of delivery information from the key facility.

26. (currently amended) The method of Claim 18, wherein the key facility is a trusted third party. ~~is the key facility.~~

27. (currently amended) A data transfer system comprising:

a key facility;

a sender facility configured to communicate with the key facility, the sender facility including a first encryption module configured to encrypt data for an intended recipient, a partitioning module configured to split the data into encrypted parts such that no part is decryptable on its own, a second encryption module configured to encrypt at least one of the parts for the key facility so as to produce a further encrypted part, a combiner configured to combine the further encrypted part and a remaining encrypted part so as to produce a data block, a signature module configured to sign the data block, and a first transmitter configured to send the data block to the key facility; and

a receiver facility configured to communicate with the key facility, the receiver facility ~~including~~ comprising a receiver configured to receive the data block from the key facility, and a command module configured to request decryption of the further encrypted part by the key facility;

wherein the key facility further comprises a receiver configured to receive the data block from the sender facility and to forward the data block to the receiver facility, a first log module configured to log recipient of the data block from the sender facility, a second log module configured to log receipt of the decryption request from the receiver facility as proof of delivery of the data block to the receiver facility, a first decryption module configured to decrypt the further encrypted part ~~on~~ after receipt of the request from the receiver facility, and a second transmitter configured to send the decrypted further encrypted part to the receiver facility;

wherein the receiver facility further comprises a second decryption module configured to decrypt the encrypted part and the decrypted further encrypted part provided by the key facility; and

wherein the sender facility further ~~includes~~ comprises a delivery module configured to request proof of delivery information from the key facility.

28. (currently amended) A data transfer system comprising:

a key facility;

a sender facility configured to communicate with the key facility and a receiver facility, the sender facility ~~including~~ comprising a first encryption module configured to encrypt data for an intended recipient, a partitioning module configured to split the data into encrypted parts such that no part is decryptable on its own, a second encryption module configured to encrypt at least one of the parts for the key facility so as to produce a further encrypted part, a combiner configured to combine the further encrypted part and a remaining encrypted part so as to produce a data block, a signature module configured to sign the data block, and a first transmitter configured to send the data block to the receiver facility;

wherein the receiver facility is configured to communicate with the key facility and the sender facility, and the receiver facility ~~includes~~ comprises a receiver configured to receive the data block from the sender facility, and a command module configured to request decryption of the further encrypted part by the key facility;

wherein the key facility further comprises a log module configured to log receipt of the further encrypted part, a first decryption module configured to decrypt the further encrypted part ~~on~~ after receipt of the request from the receiver facility, and a second transmitter configured to send the decrypted further encrypted part to the receiver facility; and

wherein the receiver facility further comprises a second decryption module configured to decrypt the encrypted part and the decrypted further encrypted part provided by the key facility.

29. (currently amended) A method of transferring data, comprising:

at a sender facility:

encrypting data for an intended recipient, splitting the data into encrypted parts such that no part is decryptable on its own, encrypting at least one of the parts for a key facility so as to produce a further encrypted part, combining the further encrypted part and a remaining encrypted part so as to produce a data block, signing the data block and sending the data block to the key facility;

at the key facility:

receiving the data block from the sender facility, forwarding the data block to the receiver facility, and logging receipt of the data block from the sender facility;

at a receiver facility:

receiving the data block from the key facility, and requesting decryption of the further encrypted part by the key facility;

at the key facility:

logging receipt of the decryption request from the receiver facility as proof of delivery of the data block to the receiver facility, decrypting the further encrypted part ~~on~~ after receipt of the request from the receiver facility, and sending the decrypted further encrypted part to the receiver facility;

at the receiver facility:

decrypting the encrypted part and the decrypted further encrypted part provided by the key facility; and

at the sender facility:

requesting proof of delivery information from the key facility.

30. (currently amended) A method of transferring data, comprising:

at a sender facility:

encrypting data for an intended recipient, splitting the data into encrypted parts such that no part is decryptable on its own, encrypting at least one of the parts for a key facility so as to produce a further encrypted part, combining the further encrypted part and a remaining encrypted part so as to produce a data block, signing the data block and sending the data block to a receiver facility;

at the receiver facility:

receiving the data block from the sender facility, and requesting decryption of the further encrypted part by the key facility;

at the key facility:

logging receipt of the further encrypted part, decrypting the further encrypted part ~~on~~ after receipt of the request from the receiver facility and sending the decrypted further encrypted part to the receiver facility;

at the receiver facility:

decrypting the encrypted part and the decrypted further encrypted part provided by the key facility.